



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/831,368	08/03/2001	Kazuhiro Aihara	108269-00005	9707

4372 7590 01/06/2005

ARENT FOX KINTNER PLOTKIN & KAHN  
1050 CONNECTICUT AVENUE, N.W.  
SUITE 400  
WASHINGTON, DC 20036

EXAMINER

PYZOCHA, MICHAEL J

ART UNIT PAPER NUMBER

2137

DATE MAILED: 01/06/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

<b>Office Action Summary</b>	<b>Application No.</b> 09/831,368	<b>Applicant(s)</b> AIHARA ET AL.	
	<b>Examiner</b> Michael Pyzocha	<b>Art Unit</b> 2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
  - If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
  - If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
  - Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 03 August 2001.
- 2a) ☐ This action is **FINAL**.                      2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 1-10 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-10 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 03 August 2001 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All    b) ☐ Some \*    c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- |  |   |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)  | 4) <input type="checkbox"/> Interview Summary (PTO-413)<br>Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)   | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152)             |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)<br>Paper No(s)/Mail Date <u>8202001</u> . | 6) <input type="checkbox"/> Other: _____  |

**DETAILED ACTION**

1. Claims 1-10 are pending.

***Claim Rejections - 35 USC § 103***

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

3. Claims 1-4, 6-10 are rejected under 35 U.S.C. 103(a) as being unpatentable over Menezes et al ("Handbook of Applied Cryptography") and further in view of Kung (U.S. 5,241,594).

As per claims 1, 9-10, Menezes et al discloses an authentication server for giving authentication to an item of data (see page 388-389), wherein the authentication server outputs encryption information (see page 389 10.3 Remark).

Menezes et al fails to disclose an intermediary server for inputting data from a terminal and distributing an encryption program to the server based on the outputted data from the application server.

Art Unit: 2137

However, Kung teaches such an intermediary server (see column 4 lines 17-29).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to use Kung's server as an intermediate between the terminal and Menezes et al's authentication server with Kung's application program as an encryption program.

Motivation to do so would have been to provide an interface to the authentication server (see Kung column 4 lines 17-29).

As per claims 2, 6, 8, the modified Menezes et al and Kung system discloses the authentication server evaluates a validity of a session given from said user terminal by comparing the second data encrypted by the encryption program with what the second data possessed by said authentication server itself is encrypted by the encryption function (see Menezes et al page 389 (ii) **"Encrypted" password files**).

As per claims 3, 7, the modified Menezes et al and Kung system discloses the encryption information changes per session to said intermediary server from said user terminal (see Menezes et al page 389 where it is inherent

Art Unit: 2137

that each session with a different user would have different encryption information).

As per claim 4, the modified Menezes et al and Kung system discloses the first data is a user's ID and the second data is a password (see Menezes et al page 388).

4. Claim 5 is rejected under 35 U.S.C. 103(a) as being unpatentable over the modified Menezes et al and Kung system as applied to claim 2 above, and further in view of Menezes et al (p. 11).

As per claim 5, the modified Menezes et al and Kung system fails to disclose the encryption information is an encryption key which specifies an encryption function.

However, Menezes et al discloses an encryption key that defines an encryption function (see page 11).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to use Menezes et al's encryption key to uniquely define the encryption function of the modified Menezes et al and Kung system.

Motivation to do so would have been to create cipher text (see Menezes et al page 11).

Art Unit: 2137

**Conclusion**

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael Pyzocha whose telephone number is (571) 272-3875. The examiner can normally be reached on 7:00am - 4:30pm first Fridays of the bi-week off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Andrew Caldwell can be reached on (571) 272-3868. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

MJP

*Andrew Caldwell*  
Andrew Caldwell